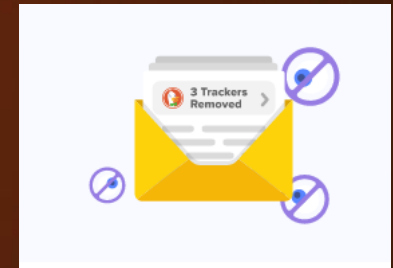
プライバシーツールを一挙紹介

JCA-NET セミナー 2023/6/20

セキュリティとプライバシー防御
個人データを営利目的、国益に利用されないために

多くのネットのユーザーにとって、検索エンジンGoogle、メールサービスのGmailやメーリングリストのGoogle Group、地図のGoogle Map、動画のYoutube

やTikTok、ブラウザのGoogle Chrome、オンライン会議のZOOMなどはごく当たり前になっています。

SNSでは、Facebook、Twitter、Instagramなどが世界標準ともいえる地位を占め、日本ではこれに加えてLineの利用が一般的になっています。また営利目的でサービスを提供している企業が、サービスそのものは無料として顧客を獲得する手段にしていることもごく当たり前に行われています。

セキュリティとプライバシー防御
個人データを営利目的、国益に利用されないために

これらのツールが選ばれる理由は、必ずしもプライバシーやセキュリティを最優先にして利用者の人権やコミュニケーションの権利を重視したサービスだから、というわけではないと思います。

- もっぱら無料で便利であることや、他の多くの人達が利用しているので、自分も利用しなければグループのコミュニケーションに加われない
- 市民運動などにとっては、より効果的な情報拡散のためにより多くのユーザーが利用しているサービスを活用することが、効率的にアピールできる

という実利的な判断もありえると思います。

セキュリティとプライバシー防御
個人データを営利目的、国益に利用されないために

他方で、プライバシーやセキュリティを重視した選択をした場合には、一般に普及しているサービスとは別の選択肢の方が好ましいばあいが多いのです。これまでもセミナーでは様々なオルタナティブなサービスやツールを紹介してきました。

- 検索エンジンの ĐuckĐuckGo
- 暗号化メールサービスの Proton や Tutanota
- オンライン会議 Jitsi-meet
- Twitter に代替する分散型 SNS の mastodon

などなど

セキュリティとプライバシー防御
個人データを営利目的、国益に利用されないために

今回は以下をテーマにします。

- 網羅的にどのようなサービスがあるのかについての鳥瞰図のようなものを提供
- 実際に自分の必要に応じてサービスを選択できるようにするための最初の手掛かりを提供
- 新たなサービスを選択するときに、便利で無料であることを最優先にぜずに、ちょっと不便であってもプライバシーやコミュニケーションの権利を優先し個人情報を売り物にしないサービスを選択することがなぜ大切なのか
- それはどうやって見分けたらいいのか、その目安について

セキュリティとプライバシー

- 第三者のアクセスを排除する
- 暗号化してコンテンツにアクセスされても内容を読むことができないようにする
- 誰が通信の主体なのかを知られないようにする
- どこから通信しているのかを知られないようにする
- 様々なデータが「自分」と関連づけられないようにする

セキュリティとプライバシー

なぜ必要なのかは、それぞれの人の事情による

- 労働運動の活動家は経営者に知られないような通信が必要
- 弁護士は依頼人を守るために、第三者に盗聴されたりデータを窃取されないことが必要
- 亡命者は出身国の情報機関などによる追跡や迫害を逃れながら通信を確保することが必要
- ジャーナリストは内部告発者の身元が暴露されないように取材することが必要
- DV の被害者は加害者からの追跡を回避しながら必要な通信を確保することが必要
- 子どもは親の過剰な干渉から自分の通信の秘密を確保することが必要

セキュリティとプライバシー

自分はセキュリティやプライバシーにこだわる特段の事情はない...という場合もあるが......

- 通信の相手もまた自分と同じ事情かどうかはわからない
- 自分にとってはさほど重要なプライバシー案件ではないと思っていても、相手にとっては深刻かもしれない
- 自分の国では「OK」だからといって相手の国でも「OK」とは限らない
- 自分の知らないところで、自分の個人情報が窃取されていても実感が伴わないので、スルーしてしまう
- ネットのセキュリティやプライバシー対策は、「苦手」なので、ついそのままにしてしまう

セキュリティとプライバシー

セキュリティはプライバシーは法律で保護されているのではないか？

確かに法律による保護はある程度はあるが ....

- 人間のプライバシー情報の多くは一生モノである。(指紋や顔、 DNA そのほかの生体情報、名前、生年月日、性別、マイナンバー ...)
- 法律は改悪されたり、解釈の変更、裁判での不利な判決などに伴う危険性が常にあり、万全ではない
- コンピュータのプログラムそのものにプライバシーや人権を保護する仕組みが組み込まれていないことが多い
- 政府は国益を優先し、企業は利潤を優先する組織であり、これらは、私たち個人の権利を守らないことがあるということを前提に考える必要がある

セキュリティとプライバシー

ネットのセキュリティやプライバシーでわからないことは、詳しいことを知っている友人がいるので、大丈夫だ ... という人もいるが ...

- ネットにおけるセキュリティやプライバシーの防衛対策を特定の個人に依存することにはリスクがある。
  - 友だちと喧嘩した
  - 遠くに引っ越して自由に会えない
  - 「旅立った」...
- 特定の個人に依存せず、「コミュニティ」として共同で相談したり問題を解決できる仕組みを作ることが必須
  - 知識の共有
  - 相互扶助

セキュリティとプライバシー

たとえば、JCA-NETのセミナーではセキュリティとプライバシーについて様々な情報を提供しています。では...

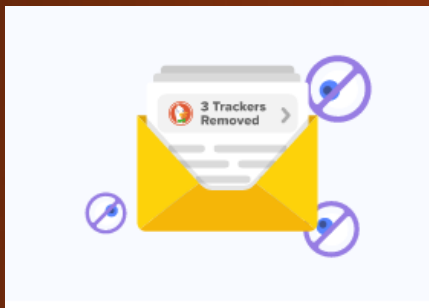
- このセミナー以外に、こうした情報を得ることはできていますか？
- 自分ひとりでセキュリティとプライバシーの防衛について、どこまで、何ができるか（逆に何ができないか）を確認したことがありますか？
- このセミナーで紹介しているソフトなどは、一般によく使われているものではありません。よくわからない、ということになれば、多くの人たちが使っているセキュリティやプライバシー上問題のあるソフトに逆戻りしかねません。

ポイントとなる考え方

- 暗号化
  - 通信経路の暗号化
  - コンテンツの暗号化
- 匿名性
  - 自分の名前、住所、性別、所属などが秘匿されている
  - 自分についての様々なデータを組み合わせても自分にたどりつかない
- オープンソース / フリーソフトウェア
  - 技術の透明性。第三者による検証が可能
  - 必要な改変ができること。自由に配付できること。

検索を google から duckduckgo に切り替えよう

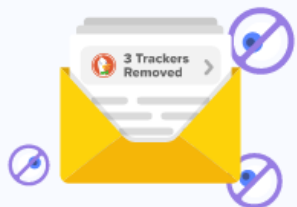
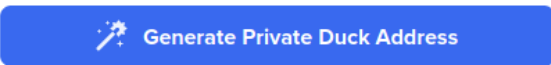
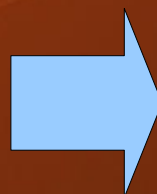
Google は、220 万以上の他のウェブサイトや 100 万以上のアプリで広告を販売しています。あなたがこれらのサイトやアプリにアクセスするたびに、google はその情報を取得してあなた向けにターゲットを絞った広告を表示するなどのビジネスを展開しています。
検索サイトを利用するときは、自分のデータを営利目的で利用しないサービスを選ぶ必要があります。DuckDuckGo は個人情報の収集や検索履歴を取得するなどをしない検索サービスです。

https://duckduckgo.com/

普段使っているメアドを知られたくないとき：DuckDuckGoMail

次のようなことはよくある。

- 買い物サイトで買い物をするときに登録するメアドを普段使っている自分のメアドにすると、そのあと余計な広告や宣伝メールが来て迷惑することがある
- メアドは知られたくない相手にメールで連絡をとる必要がある
- 防衛省、NATO、米国国防総省などが配信しているメールニュースを購読したいが、自分のメアドを登録するのは不安だ
- イベントの問い合わせメールを作りたい

ĐuckĐuckGoMailは、こうした場合に利用できるメールアドレス生成サービス。

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/duckduckgo_protect-your-inbox-with-duckduckgo-email-protection_faq/

普段使っているメアドを知られたくないとき：DuckDuckGoMail

可能な限り足跡を残さずウェッブへのアクセスを可能に

ウエッブにアクセスするたびに、私たちの実感できない仕組みを使って多くのデータを把握するだけでなく、これを第三者とも共有することが問題になっています。第三者クッキーと呼ばれる仕組みはその代表格で、各国政府も規制のルールを策定しはじめています。ところが、こうした問題はクッキーだけではなく、「フィンガープリント」とよばれるもっと厄介かもしれない仕組みもあります。Mullvadというブラウザはこのフィンガープリントを極力取得させないような設計を取り入れています。

プライバシーポリシー

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/mullvad_privacy-policy_jp/

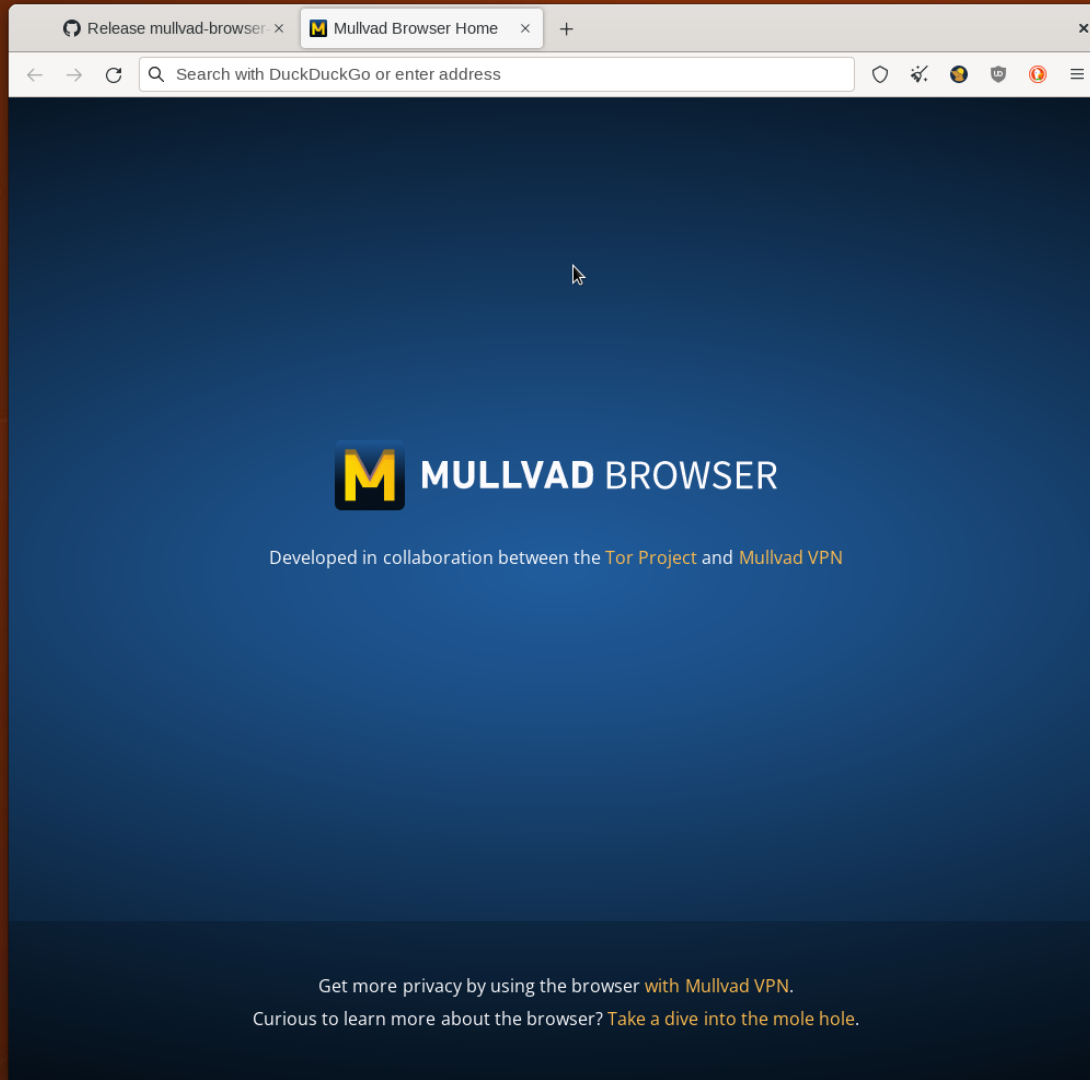
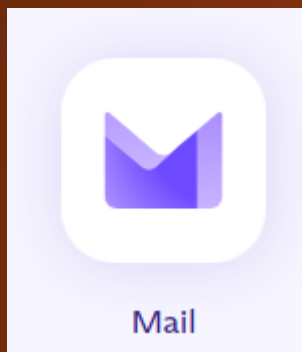
可能な限り足跡を残さずウェッブへのアクセスを可能に

Release mullvad-browser × | Mullvad Browser Home ×

Search with DuckDuckGo or enter address

MULLVAD BROWSER

Developed in collaboration between the Tor Project and Mullvad VPN

Get more privacy by using the browser with Mullvad VPN.
Curious to learn more about the browser? Take a dive into the mole hole.

EFF の https://coveryourtracks.eff.org/ でのチェックでは、特に顕著な違いを見出せなかったが....。今後を期待したいです。

メールのプライバシーを守るなら「暗号化メール」を使おう

メールは郵便でいえば「ハガキ」です。あなたが契約しているインターネットのプロバイダーやGmail、Yahooメールのようなメールサービスの会社はあなたのメールボックスを覗くことができます。メールのプライバシーに配慮することはあなたの通信相手のプライバシーに配慮することでもあります。とくに人権問題などの活動をしている場合、メールのプライバシー保護は必須です。Protonmail や Tutanota など、メールを暗号化して保管するサービスがあります。これらを使うことでプロバイダーなどの「盗聴」を防ぐことができます。（ただし、送受信者双方が暗号化サービスを使う必要があります）

Protonmail https://proton.me/

Tutanota https://tutanota.com/ja/

Line でいいの？プライバシーを守るなら Signal の方がずっといい！

友人や家族、職場の仲間、なじみの飲み屋、それに行政の案内までみな Line でお友達繋りが普通になっています。Line は 2022 年上半期だけで 1500 件の情報を捜査機関に開示しています。Signal は、すべてのメッセージを暗号化してやりとりできるアプリです。Signal の運営サイドを含む他の誰も、メッセージを盗み読みしたり通話を傍受できません。Signal では、すべてのメッセージと通話が常に暗号化されます。

https://signal.org/ja/

Line でいいの？プライバシーを守るなら Signal の方がずっといい！

Line から Signal へ
https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/line_to_signal/
Signal のダウンロードとインストール
https://signal.org/ja/download/

Signal よりいい？電話番号、メアドなしで OK

個人対個人、グループで使えるプライベートなメッセージングアプリ。Signal では、利用に電話番号が必要になるが、Session は電話番号もメールアドレスも不要。一切の個人情報なしで使えるように設計されています。日本も含めて多くの国では電話番号の登録に身分証明が必要なため、番号を用いたアプリ利用の方法は、番号から個人を特定されるリスクがあります。Session は、個人を特定できない SessionID と呼ばれる特殊な ID を使って通信することができます。通信経路に onion の仕組みを導入することで IP アドレスから発信元を特定されない工夫がされています。

https://getsession.org/

※スマホが盗まれたり押収されてログインパスワードを解読された場合、Session に容易にアクセス可能になる恐れがあります。

Signal よりいい？電話番号、メアドなしで OK

(Session) プライバシーポリシー
https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/session_privacy_polivy_jp/

(privacyaffairs.com)Session App のレビュー： 知っておくべきことのすべて
https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/privacyaffairs-com_session-app_jp/

パス

Session は、Sessionの分散型ネットワークの複数のサービスノードを介してメッセージをバウンスすることにより、IP を隠します。以下は現在接続がバウンスされている国です。

デバイス
South Africa
Germany
United States
保存先

さらに詳しく

ドキュメントの共有、アンケートや日程調整 ...Cryptpad という優れものがある！

皆で文章を校正したり、会議の日程を相談したり、アンケートのフォームを設置したり、こうした作業を Google のサービスに頼ることがありますが、これらを暗号化して安全に保護しながら実現してくれるサービス、Cryptpad があります。
CryptPad 上のすべてのデータは、ブラウザーで暗号化されます。Signal 同様サービス管理者でさえ、ドキュメントの内容やユーザー データを見ることはできません。

https://cryptpad.org/

ドキュメントの共有、アンケートや日程調整 ...Cryptpad という優れものがある！

料金　ドキュメンテーション　toshi

CryptPad.fr

エンドツーエンド暗号化オープンソースコラボレーションスイート「CryptPad」の公式インスタンスです。CryptPad 開発チームによって管理されています。

暗号化されたデータはフランスに保存されています。

利用規約　プライバシーポリシー　連絡先

新しいドキュメント

スプレッドシート　リッチテキスト　カンバン

コード　フォーム　ホワイトボード

マークダウンスライド

ドライブ

より多くのストレージ容量が必要な場合：

定額利用を申し込む

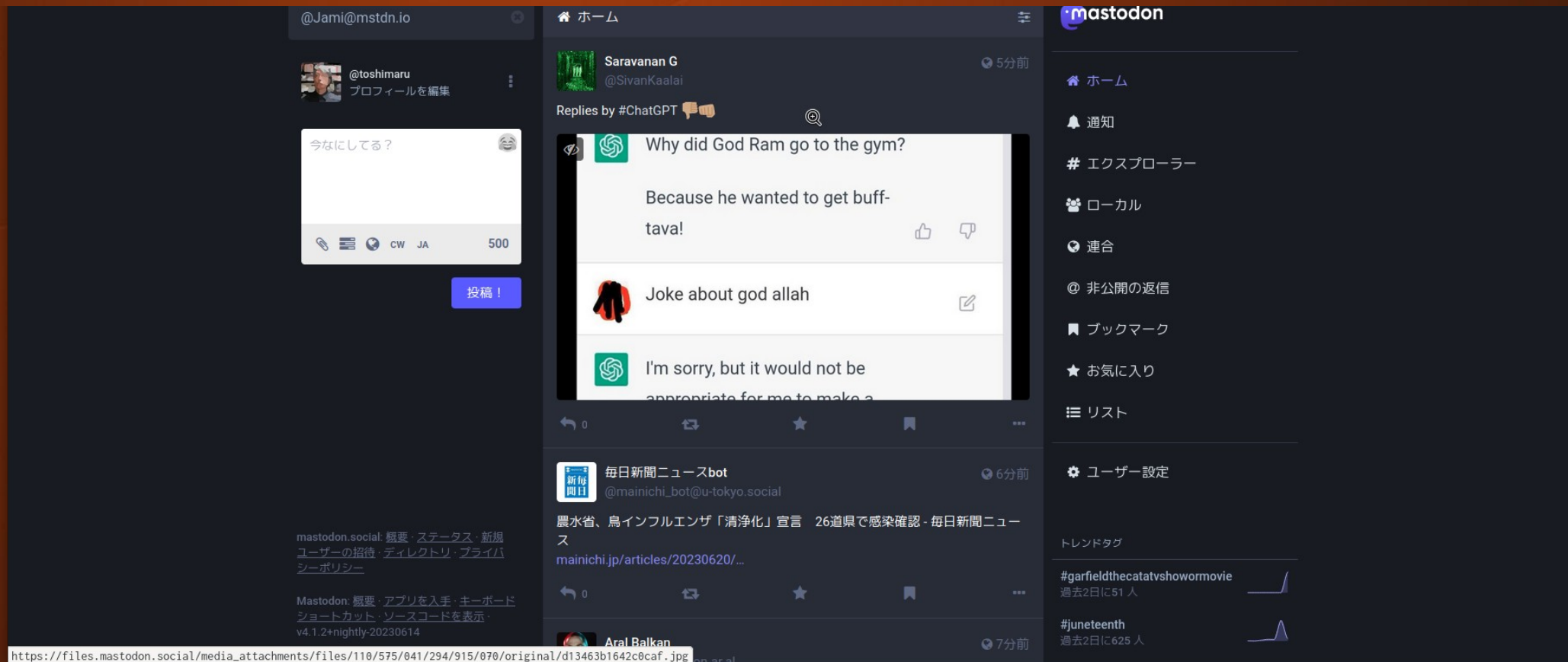
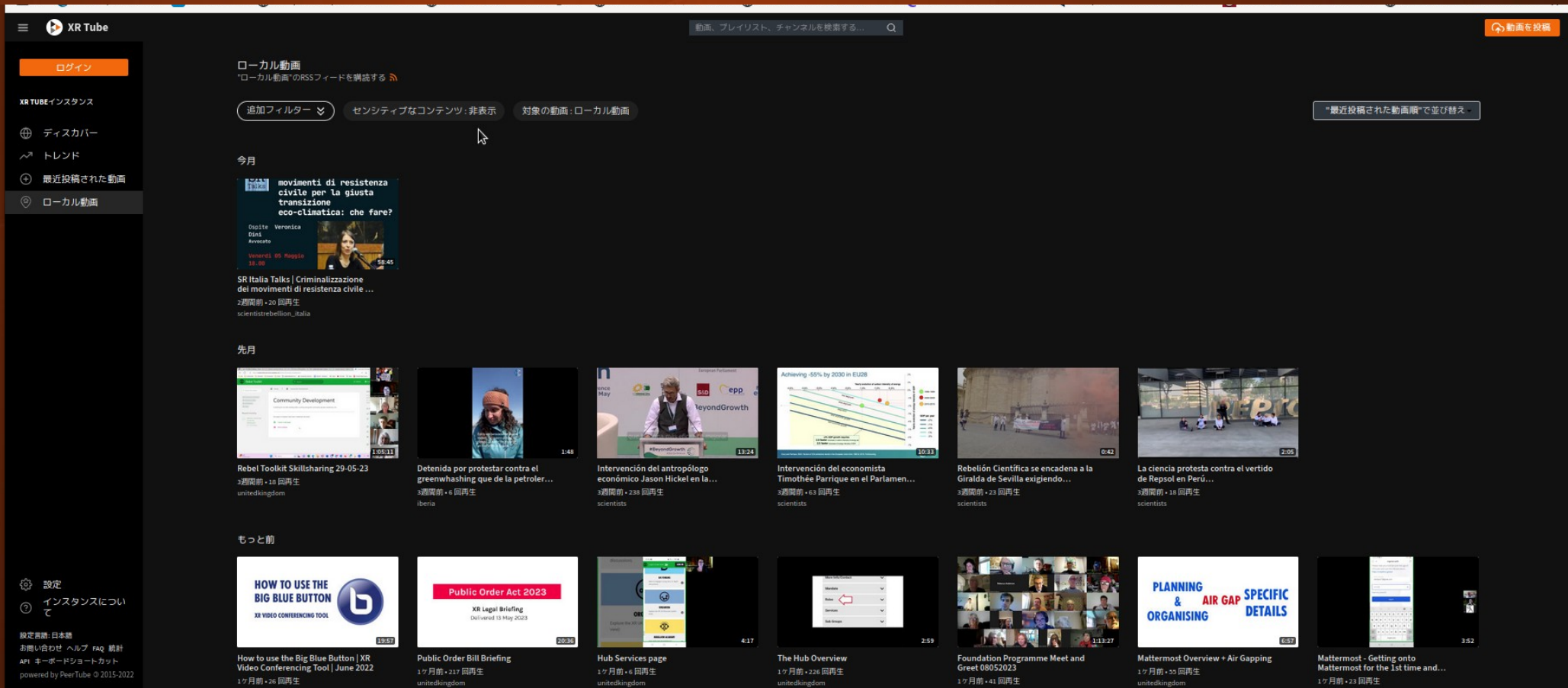
mastodon

イーロン・マスク独裁のTwitterから連合型のMastodonに乗り換える

Twitterは膨大なユーザーをかかえて拡散力の大きなSNSですが、営利企業のサービスが経営者の判断に大きく影響されることをイーロン・マスクの横暴な振舞いで実感した人も多く、Twitterから離れる人達がでてきています。その受け皿のひとつがMastodonです。Masotdonは特定の企業の運営するものではなく、独立したサーバーが相互に連携してネットワークを組むフェディバースという仕組みを使っています。ヘイトスピーチなど不愉快なメッセージを目にしなくてもいい仕組みにもなっています。「売り物ではないソーシャルネットワークサービス」をスローガンにしています。

https://joinmastodon.org/ja

イーロン・マスク独裁のTwitterから連合型のMastodonに乗り換える

小倉のmastodonのページ
https://mastodon.social/@toshimaru

Youtube の動画配信支配に挑戦する非中央集権型サービス

mastodon と同じ連合型の仕組みをとる動画配信のサービス。「ビッグテックによる、動画プラットフォームからの脱却」をスローガンにしています。

- Peertube のサイトは誰でも自分のサーバーに設置できるので、 Youtube のような統一したポリシーに拘束されることありません。
- PeerTube はサーバー同士を連合することで、独立しながら、相互接続された巨大なネットワークの輪を構成しています。
- PeerTube はいかなる広告に依存せず、ユーザーを追跡したりもしません。

https://joinpeertube.org/

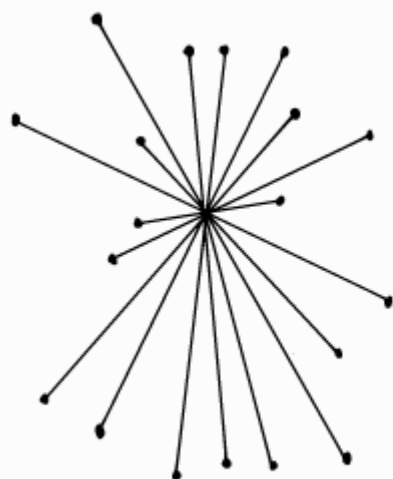
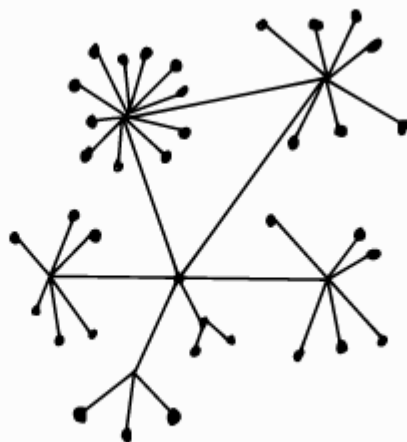
Youtube の動画配信支配に挑戦する非中央集権型サービス

上は、 Peertube のイギリスの反気候危機運動団体、 Extinction Rebellion のサイト
https://tube.rebellion.global/

20～30人までならZOOMでなくてもJitsiでいいと思う

オンライン会議室のことを「ZOOM」と呼ぶことが一般的になってしまいました。企業のマーケティングでいうと、自社のブランドが普通名詞として通用するようになると、多くの人達が、意識せずに、ブランドの宣伝の担い手になってしまいます。
ZOOMのサーバーが利用者の会議の様子をどの程度把握できるのかはわかりません。しかし、ZOOMの会議が、その内容(天安門事件、パレスチナ解放闘争)によって遮断されたことがあります。他方、Jitsiの設計図は公開されており、誰でもサーバーにインストールして使えます。信頼できるサーバーを捜して使うことはセキュリティやプライバシーにとって重要なこと。https://meet.jit.si/

サーバーに依存しない オンライン会議室

Jami は完全に Peer to Peer で通信が行われるため、ユーザー間でデータを中継するためのサーバーは必要ない
全ての会話は Peer to Peer および End to End で暗号化されています。
アカウントの作成に個人情報を提供する必要ありません。

左図のように、Jami には、サーバーなしで、参加者を繋ぐ仕組みになっています。
https://jami.net/

ZOOM　Jitsi　Jami

ワード、エクセル、パワポと口にするたびに、あなたはMSの広告塔になっている

LibreOfficeは、The Document Foundationという非営利組織のプロジェクトでコミュニティベースでフリーソフトウェアの原理を信じ、そしてその成果を制限のない形で世界中で共有することを信じるユーザーによって開発されています。マイクロソフト社のオフィス製品のような企業が独占するソフトウェアとは真逆の姿勢をとっています。

- 私たちのオフィススイートに対し制限されないアクセスを無償で提供する
- 私たちのソフトウェアを各自の言語で翻訳し、文書化し、そしてサポートすることを奨励する
- オープンな標準とフリーソフトウェアを、オープンかつ透過的なピアレビュープロセスを通じて作成し開発することを促進させ、その活動に活発に参加する

文書作成、表計算、プレゼンテーション、ちらし作成などほとんどのことができます。https://ja.libreoffice.org/

地図といえばGoogle Mapですか？Open Street Mapの方がおもしろいと思うけど...

OpenStreetMapは、道路、通路、カフェ、鉄道駅など、世界中にあるすべてのものに関するデータを提供・メンテナンスしているマッパーのコミュニティによって構築されています。

協力者は航空写真やGPS機器、ローテクのフィールド地図を使用して、OpenStreetMapが正確で最新の状態であることを確認しています。

OpenStreetMapはオープンデータ。利用者はOpenStreetMapと協力者の著作権を表示すれば、いかなる目的にも無料で利用することができます。もし何らかの方法でデータを変更したり二次データを作成したりした場合も、同じライセンス条件下で結果を配布できます。

https://www.openstreetmap.org/

プライバシー重視でオープン/フリーなソフトウェアを使うこと自体がライフスタイルを変える運動になる!!

本日紹介したソフト以外にも多くのソフトがあります。私たちが、日常的な仕事や市民運動、労動運動などの活動で、Line や Gmail を使ったり Twitter を使ったり、パワポでプレゼンしたり、ワードでデータを交換したりすることは「便利」ですが、同時に、これらにやや不安を感じている人達がいたとしても「あの人たちが使っているのだから私たちも使っていいのだ」という間違ったメッセージを発信してしまうかもしれません。

オープンソース/フリーソフトウェアを使うこと、プライバシーやセキュリティを重視するソフトを使うことは、道具の選択の優先順位で何が一番大切なことなのかを、多くの皆さんに実践で示すという意味があります。このことの意味は大きいのです。ぜひ、このことを考えながら、仲間の皆さんと、ライフスタイルを変える工夫にチャレンジしてみてください。